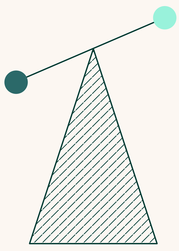
segura | Futureproof Identity Security

INFOGRAPHIC

PAMaturity Framework



The Segura PAMaturity Framework is a proprietary model designed to help organizations evaluate, benchmark, and evolve their Privileged Access Management (PAM) capabilities.

Built around nine strategic pillars, the framework enables a holistic and practical maturity ssessment—covering not only technology, but also governance, integration, and business alignment.

The PAMaturity Framework guides maturity evaluations, identifies quick wins, and shapes multi-phase PAM roadmaps.

Maturity Levels

- **0- Ad Hoc:** No formal PAM strategy; unmanaged privileged accounts.
- **1- Initial:** Some manual processes or basic vaulting, but lacking consistency.
- **2- Developing:** Tool-based management for selected systems; basic visibility and some policy controls.
- **3- Defined:** Broader scope; policies aligned with least privilege; vaulting and session monitoring in place.
- **4- Managed:** JIT access, automated workflows, remote access coverage, integrated risk-based controls.
- **5- Optimized:** Continuous risk scoring; full coverage (on-prem/cloud); integrated CIEM/IGA; AI-driven analytics.

Maturity Indicators

Pillars of Assessment	0-1	2-3	4-5
Governance & Strategy **a.** Is there executive sponsorship and clear ownership of PAM? **b.** Is there a strategic roadmap aligned with security goals? **c.** Are policies defined for privileged access and lifecycle management? **d.** Are there KPIs or metrics to measure PAM effectiveness and maturity? **e.** Is there resistance to change or a lack of awareness about PAM's importance?	No dedicated PAM governance; PAM treated as a tool, not a program.	PAM embedded in enterprise IAM strategy; periodic reviews and risk-based policy updates.	Documented policies; initial role-based access and enforcement.
Account Discovery & Inventory **a.** Is there an up-to-date inventory of all privileged accounts (human and non-human)? **b.** Are privileged accounts automatically discovered across all environments (cloud, on-prem, hybrid)? **c.** Are privileged accounts regularly audited for ownership and necessity? **d.** Are orphaned or unused accounts promptly decommissioned? **e.** Is account discovery integrated with asset management and IGA tools?	Privileged accounts are untracked.	Periodic manual discovery; partial automation.	Continuous discovery; full asset and user mapping across hybrid environments.
Access Control & Just-in-Time (JIT) Privileges **a.** Do administrators have standing access or is it issued only when needed? **b.** Is access granted through policy-based approvals? **c.** Is the principle of least privilege enforced systematically? **d.** Is JIT access implemented for all or most critical systems? **e.** Are elevation requests audited and reviewed?	Admin rights are always on.	Role-based access with some delegation.	JIT elevation; zero standing privileges; policy-based access control.
Credential & Secrets Management **a.** Are privileged credentials stored securely (e.g., in a vault)? **b.** Are credentials automatically rotated on a regular basis? **c.** Is access to shared credentials controlled and monitored? **d.** Are secrets managed programmatically for DevOps, applications, and scripts? **e.** Are there policies for managing hardcoded secrets and API keys?	Passwords stored in files or known by users.	Centralized vault with manual rotation.	Automated credential rotation; secrets management integrated with DevOps.
Session Management & Monitoring **a.** Are privileged sessions recorded and monitored? **b.** Can anomalous behavior during privileged sessions be detected and alerted? **c.** Are session logs retained in accordance with compliance requirements? **d.** Are remote privileged sessions brokered (i.e., no direct connections)? **e.** Can session data be used for forensic analysis?	No monitoring or logging in place.	Session recording on sensitive systems.	Real-time monitoring with behavior analytics and anomaly detection.
Integration & Automation **a.** Is PAM integrated with identity governance, ITSM, SIEM, and CMDB? **b.** Are onboarding/offboarding processes for privileged access automated? **c.** Are PAM processes orchestrated through workflows (e.g., ticketing, approvals)? **d.** Can the PAM platform trigger security automation or remediation actions? **e.** Are APIs used to extend PAM capabilities across environments?	Siloed solutions with no integrations.	Some API-based integrations in place.	Full automation; integration with SIEM, IGA, ITSM tools.
User Behavior & Risk Analytics **a.** Is privileged user activity analyzed for risk indicators? **b.** Are machine learning or UBA (User Behavior Analytics) used to detect anomalies? **c.** Are risky behaviors (e.g., off-hours access) flagged automatically? **d.** Are risk scores used to influence access decisions? **e.** Are metrics and KPIs in place to evaluate PAM effectiveness?	No behavior-based insights.	Manual reviews of privileged activity.	AI/ML-driven analytics and continuous risk scoring.
Cloud & Remote Access Coverage **a.** Is cloud infrastructure (IaaS, PaaS, SaaS) protected by PAM controls? **b.** Are remote sessions secured without VPNs (e.g., via RPAM)? **c.** Are third-party vendor sessions governed and monitored? **d.** Is CIEM integrated or used alongside PAM for cloud entitlements? **e.** Are unmanaged devices blocked from initiating privileged access?	No behavior-based insights.	Manual reviews of privileged activity.	AI/ML-driven analytics and continuous risk scoring.
Compliance & Policy Enforcement **a.** Are auditable policies in place governing privileged access? **b.** Are policies enforced through automation (e.g., access expiration)? **c.** Are separation of duties (SoD) rules applied to prevent conflicts of interest? **d.** Are compliance reports automatically generated from PAM data? **e.** Are audit findings (internal and external) consistently addressed?	Reactive response to audits.	Basic policy templates and enforcement.	Continuous compliance monitoring; fine-grained SoD and policy enforcement.

About Segura

Segura is a leading provider of innovative Privileged Access Management (PAM) solutions, dedicated to helping organizations safeguard their critical digital assets. With a strong commitment to security and customer success, senhasegura has become a trusted partner for organizations worldwide looking to enhance their cybersecurity posture.

Our state-of-the-art PAM platform offers a comprehensive suite of advanced security features, including access management, credential management, session management, and privileged user analytics. Designed to be highly customizable and easily integrated with existing IT infrastructures, senhasegura's PAM solution ensures a seamless implementation process and ongoing support.

By choosing Segura, your organization can confidently protect its most valuable assets and thrive in the face of ever-evolving cyber threats.